Buffalo Law Review

Volume 62 | Number 5 Article 5

12-1-2014

Snap and Destroy: Preservation Issues for Ephemeral Communications

Ryan G. Ganzenmuller
University at Buffalo School of Law (Student)

COMMENT

Snap and Destroy: Preservation Issues for Ephemeral Communications

RYAN G. GANZENMULLER†

INTRODUCTION

In an Internet age where "delete" no longer means "gone forever," the desire for short-lived communications has risen.[1] The founder of Wickr, a mobile application for impermanent media, opined that "[e]phemeral data is the future."[2] This is supported by the meteoric rise of Snapchat, the self-destructing photo application that has grown into a startup valuated at an estimated $10 billion just three years after its founding.[3] While Snapchat thrives in younger

---

† Editor-in-Chief, *Buffalo Law Review*; J.D. Candidate, 2015, SUNY Buffalo Law School; B.A., 2012, Binghamton University. Special thanks to Professor Christine Bartholomew for her invaluable guidance on this Comment and throughout law school. Thanks also to Professor Mark Bartholomew for his advice and to Anna Kreiter and Brooke Leone for critiquing my draft. I am grateful for the love and support of my family and friends, especially the ones who sent me countless Snaps to inspire this Comment. Finally, thanks to the *Buffalo Law Review* members for their efforts, my Editorial Board members for their unending hard work and dedication, and Erin Connare for her editorial work on this Comment.

1. John G. Browning, *Burn after Reading: Preservation and Spoliation of Evidence in the Age of Facebook*, 16 SMU SCI. & TECH. L. REV. 273, 275, 306 (2013) [hereinafter Browning, *Burn after Reading*]; Felix Gillette, *Snapchat and the Erasable Future of Social Media*, BLOOMBERG BUSINESSWEEK (Feb. 7, 2013), http://www.businessweek.com/articles/2013-02-07/snapchat-and-the-erasable-future-of-social-media.

2. Gillette, *supra* note 1.

3. Serena Saitto, *Snapchat Said to Close Yahoo Funding, Still Raising Money*, BLOOMBERG (Oct. 22, 2014), http://www.bloomberg.com/news/2014-10-22/snapchat-said-to-close-yahoo-funding-still-raising-money.html. This valuation

demographics,[4] Vaporstream is making a name for itself among corporate elites who wish to communicate discreetly with vanishing messages.[5] Apps for "exploding" communications are appearing one after another, showing no signs of slowing down.[6]

The proliferation of these services demonstrates a shift in how we wish to connect with one another, and more importantly, the trail we leave behind in doing so.[7] For parties involved in litigation, there is reason to be mindful of social media. One study found eighty-one percent of surveyed matrimonial attorneys had discovered and used social networking evidence in cases.[8] Attorneys in products liability, personal injury, criminal, employment, intellectual property, defamation, insurance, and securities litigation have all reported finding crucial case information on social media sites.[9] Across the country, courts have made preservation rulings on cases in which Facebook users have strengthened profile privacy settings, changed default profile pictures, deleted wall posts, deactivated accounts, and even sent taunting messages to opposing counsel.[10] Additionally, one survey found fifty-seven percent of all application users

---

figure rose to $10 billion after being valuated at an estimated $4 billion less than one year earlier. Evelyn M. Rusli & Douglas MacMillan, *Snapchat Mulls Raising Money at $3 to $4 Billion Valuation*, WALL ST. J. BLOG (Oct. 25, 2013), http://blogs.wsj.com/digits/2013/10/25/snapchat-mulls-raising-money-at-3-4-billion-valuation.

4. Nicole A. Poltash, Comment, *Snapchat and Sexting: A Snapshot of Baring Your Bare Essentials*, 19 RICH. J.L. & TECH. 14, ¶ 16 (2013).

5. *See* Browning, *Burn after Reading*, *supra* note 1, at 307.

6. *See id.* at 306-07; *see, e.g.*, Jay Yarow, *There's A New App That Lets People Send Self Destructing Messages. It Wants To Be Snapchat For Professionals*, BUSINESS INSIDER (Jan. 8, 2014, 10:47 AM), http://www.businessinsider.com/confide-a-snapchat-for-professionals-2014-1.

7. *See* Woodrow Hartzog, *The Second Wave of Global Privacy Protection: Social Data*, 74 OHIO ST. L.J. 995, 1016-17 (2013).

8. John G. Browning, *Digging for Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU SCI. & TECH. L. REV. 465, 467 (2011).

9. *Id.*

10. Browning, *Burn after Reading*, *supra* note 1, at 285-86, 291-305.

have installed, uninstalled, or declined to install an "app" due to privacy concerns.[11]

The tipping point may have been recent revelations about the National Security Agency (NSA) and its domestic surveillance operations.[12] Whistleblower Edward Snowden revealed that the NSA conducts highly invasive surveillance on American citizens and others, collecting more personal and private information than the public knew.[13] The outcry was monumental, as the extent of the United States' privacy-unfriendly exploits was previously undisclosed.[14] As one author poignantly stated, "[t]hat was then: we are all on notice now."[15]

Given this background, it is not difficult to see why self-destructing communication technologies have spiked and made it "easier for a person's bad decisions to vanish into thin air."[16] One author writes that "Snapchat's self-destructing messages make users feel immune from repercussions."[17] A study found that seventy-seven percent of college students use Snapchat once per day.[18] As of October 2014, Snapchat

---

11. Gillette, *supra* note 1.

12. *See* A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965, 978-79 (2013).

13. *See id*.

14. *See id*; *see also* Heather Kelly, *Protests against the NSA spring up across U.S.*, CNN (July 5, 2013), http://edition.cnn.com/2013/07/04/tech/web/restore-nsa-protests; Bart Jansen & Carolyn Pesce, *Anti-NSA rally attracts thousands to march in Washington*, U.S.A. TODAY (Oct. 26, 2013), http://www.usatoday.com/story/news/nation/2013/10/26/nsa-dc-rally/3241417.

15. Froomkin, *supra* note 12, at 994.

16. Browning, *Burn after Reading*, *supra* note 1, at 306.

17. Poltash, *supra* note 4, ¶ 38. Poltash's article is the only article to date written exclusively about Snapchat's relation to the law, specifically regarding sexting. Accordingly, it has been cited frequently, including reference in several Virginia statutes. *See, e.g.*, VA. CODE ANN. §§ 18.2-152.7:1, 18.2-216.1, 18.2-390, 22.1-70.2, 22.1-279.6, 42.1-36.1.

18. *See* Kurt Wagner, *Study Finds 77% of College Students Use Snapchat Daily*, MASHABLE (Feb. 24, 2014), http://www.mashable.com/2014/02/24/snapchat-study-college-students.

users were sending 700 million images per day.[19] Vaporstream's website boasts that its clandestine communications are "no different than talking face-to-face over lunch or at the water cooler."[20] Other apps such as Wickr, Gryphn, TigerText, Burn Note, and Ansa use encryption to send self-destructing texts, videos, images, and documents.[21] On January 8, 2014, as this Comment was being written, a new app was unveiled called Confide; its founders touted it as the "professional counterpoint to Snapchat."[22] On January 24, 2014, another Snapchat-like app appeared called Secret Square, founded by a Vaporstream executive.[23] On May 13, 2014, Yahoo purchased a self-destructing mobile messaging startup named Blink for an undisclosed amount.[24] Paired with Facebook's highly publicized failure to acquire Snapchat—twice[25]—it is clear the big players in the tech

19. Saitto, *supra* note 3. This figure has doubled since October 2013, when users were sending 350 million images per day. Micah Schaffer, *Who Can View My Snaps and Stories*, SNAPCHAT BLOG (Oct. 14, 2013, 11:23 AM), http://blog.snapchat.com/post/64036804085/who-can-view-my-snaps-and-stories.

20. FAQ, VAPORSTREAM, https://www.benegourmet.com/faq (last visited Sept. 29, 2014) [hereinafter *Vaporstream FAQ*] (copies on file with *Buffalo Law Review*). Sometime after this Comment was written in early 2014, Vaporstream changed its entire website and, curiously, removed nearly all of the controversial language cited throughout this Comment. The website cited above preserved the older version of the website. *Compare Vaporstream FAQ*, *supra*, *with* FAQ, VAPORSTREAM, https://www.vaporstream.com/faq (last visited Sept. 29, 2014).

21. Browning, *Burn after Reading*, *supra* note 1, at 306-07; Belinda Luscombe, *TigerText: An iPhone App for Cheating Spouses?*, TIME (Feb. 26, 2010), http://content.time.com/time/business/article/0,8599,1968233,00.html; *Burning Questions: Privacy Info From Burn Note*, BURN NOTE, http://info.burnnote.com/about (last visited Feb. 6, 2014) [hereinafter *Burning Questions*].

22. Yarow, *supra* note 6.

23. Edward Cox, *Northwestern alum creates Snapchat-like app*, DAILY NORTHWESTERN (Jan. 26, 2014), http://dailynorthwestern.com/2014/01/26/campus/northwestern-alum-creates-snapchat-like-app.

24. Benjamin Horney, *Yahoo Buys Self-Destruct Mobile Messaging App Blink*, LAW360 (May 14, 2014. 1:18, PM), http://www.law360.com/articles/537699/yahoo-buys-self-destruct-mobile-messaging-app-blink.

25. First, Snapchat CEO Evan Spiegel declined a $1 billion offer from Facebook CEO Mark Zuckerberg, as Snapchat valued its worth at closer to $3 to $4 billion. *See* Rusli & MacMillan, *supra* note 3 and accompanying text. Then, when Zuckerberg offered Spiegel $3 billion, Spiegel rebuffed that as well, reportedly infuriating Zuckerberg. *See* Seth Fiegerman, *Snapchat CEO Reveals Why He*

market want to venture into this field. The futuristic 1960s *Mission: Impossible* messages that would "self-destruct in five seconds" have not only become a reality, but are now in exceedingly high demand.[26]

In fact, the demand has become so great that almighty Apple is integrating ephemeral technology into its products. In unveiling the newest iPhone operating system, iOS 8, Apple announced that all audio, photo, and video iMessages[27] will vanish unless users change the settings.[28] Users can choose self-destruct settings just like Snapchat.[29] Further, Apple redesigned its messaging and camera interfaces to compete with the easy use of Snapchat.[30] Apple marketed the feature as a means of saving phone memory, but many view this as "clearly an assault on Snapchat."[31] Regardless of the motive, hundreds of millions of iPhone users worldwide will all soon have an ephemeral data device in their pockets—a tool for "selfie-destruction"—and they will not have to go to the AppStore[32] to get it.

Rejected Facebook's $3 Billion Offer, MASHABLE (Jan. 6, 2014), http://mashable.com/2014/01/06/snapchat-facebook-acquisition-2; Evelyn M. Rusli & Douglas MacMillan, *Snapchat Spurned $3 Billion Acquisition Offer from Facebook*, WALL ST. J. BLOG (Nov. 13, 2013, 1:43 PM), http://blogs.wsj.com/digits/2013/11/13/snapchat-spurned-3-billion-acquisition-offer-from-facebook. Thereafter, Zuckerberg even attempted to "crush" Snapchat by releasing a similar app called Poke, which failed embarrassingly. *See* Fiegerman, *supra*; *see also* Mark Milian, *Zuckerberg's Snapchat Envy Isn't Disappearing*, BLOOMBERG (Aug. 14, 2014), http://www.bloomberg.com/news/2014-08-14/zuckerberg-s-snapchat-envy-isn-t-disappearing.html.

26. *See* Browning, *Burn after Reading*, *supra* note 1, at 308.

27. iMessages are communications sent between one or more iMessage-enabled iPhones. Apple's new ephemeral technology will apply only to these messages. Jacob Kleinman, *Apple Takes on Snapchat with Self-Destructing Messages in iOS 8*, TECHNOBUFFALO (June 2, 2014), http://www.technobuffalo.com/2014/06/02/apple-takes-on-snapchat-with-self-destructing-messages-in-ios-8.

28. Brandon Griggs, *Big Changes Coming to iPhone Messaging*, CNN (June 3, 2014), http://www.cnn.com/2014/06/03/tech/mobile/apple-messages-app/index.html?hpt=hp_t2; Kleinman, *supra* note 27.

29. *See* Kleinman, *supra* note 27.

30. *Id.*

31. *See id.*

32. The AppStore is Apple's highly regulated smartphone application marketplace, where users can download apps like Snapchat, Wickr, and the like.

The downside of such growth, however, is the propensity for such services to be used for illegal activity.[33] Some sign up for ephemeral data apps because they know preserved data would be a problem as they go about their dirty deeds. That incriminating "selfie"[34] you took? Good thing you used Snapchat.[35] That insider trading tip you sent? Thank God for Vaporstream.[36]

As is often the case, the law is lagging behind these advancements in technology.[37] While the applicable Federal Rules of Civil Procedure have been amended to keep up with some technological developments, the old rules never contemplated a situation in which, by design, discoverable information could disappear without a trace. This is unlike standard spoliation, where parties destroy evidence themselves.[38] This is different than merely deleting a discoverable Facebook post.[39] Here, evidence destroys itself because the party chooses a self-destroying data program to communicate.[40]

So what happens when you bring together an antiquated set of rules designed to preserve evidence for parties, and applications designed to eradicate evidence for their opponents? Could mere use of Snapchat or Vaporstream constitute spoliation? These issues become even more complex with the latest wrinkles in Snapchat's software. While Snapchat recipients have always been able to screenshot an image in order to preserve it, now users have

---

33. *See* Browning, *Burn after Reading*, *supra* note 1, at 308; Poltash, *supra* note 4, ¶¶ 21-22.

34. A "selfie" is a photograph one takes of oneself. The explosion of social media caused usage of the new term to skyrocket, earning it a place in the dictionary and the honor of being 2013 Oxford Word of the Year. *See* Ben Brumfield, *Selfie named word of the year for 2013*, CNN (Nov. 20, 2013, 12:29 AM), http://www.cnn.com/2013/11/19/living/selfie-word-of-the-year.

35. *See* Browning, *Burn after Reading*, *supra* note 1, at 306.

36. *Id.* at 307-08.

37. *Id.* at 308.

38. *See id.* at 274-75.

39. *See id.* at 295-97.

40. *See id.* at 275.

the power to save Snaps before sending them, as well as the ability to replay one received Snap per day.[41] These changes may alleviate some preservation issues associated with Snapchat. However, no cases have yet dealt with Snapchat, Vaporstream, or other self-destroying messaging apps.

Further complicating matters, what if ephemeral messages never truly disappear? Snapchat claims that once a Snap is viewed, it is deleted from Snapchat servers and recipient devices.[42] However, when Android users found ways to access old Snaps, the Electronic Privacy Information Center (EPIC) filed a complaint to the Federal Trade Commission (FTC) for deceptive business practices, criticizing Snapchat's false promises of true ephemerality.[43] Further, an app called Snaphack allegedly allows users to view old Snaps.[44] Would this change the debate? Does it matter that the sender intended for the content to never be seen again? Additionally, new technology often faces security risks, a problem that may be even worse for ephemeral media because of its deliberately disappearing nature.[45]

This Comment bridges the gap between preservation of evidence and data that are not meant to be preserved. While one article has addressed preservation issues with deleted social media posts generally[46] and some case law has dealt

---

41. *Snapchat Privacy Policy*, http://www.snapchat.com/privacy (last updated May 1, 2014).

42. *Id.*

43. *See* Joyce E. Cutler, *Privacy Group Asks FTC to Investigate Snapchat's Claims Regarding Photo Deletion*, BLOOMBERG BNA SOC. MEDIA LAW & POL. REP., May 21, 2013 [hereinafter Cutler, *Privacy Group*].

44. Kalyani M., *Snaphack App Lets You Save Snapchats Without Notifying the Sender*, SPIDEROAK BLOG, https://spideroak.com/privacypost/cloud-security/snaphack-app-lets-you-save-snapchats-without-notifing-the-sender (Nov. 21, 2013).

45. It stands to reason that if a person deliberately chooses a self-destructing communication medium, the person does not want the message to be seen by others—which suggests an outsider may be more likely to want access to such forbidden content.

46. *See* Browning, *Burn after Reading*, *supra* note 1.

with preserving certain types of temporary data,[47] no article or case has yet discussed the discovery consequences of ephemeral technologies such as Snapchat and Vaporstream. This Comment attempts to resolve the application of older legal discovery concepts to novel self-destroying technologies.

Part I explains the history of ephemeral communication applications such as Snapchat and Vaporstream and how the programs work. Part II details preservation and spoliation in electronic discovery, including current rules and interpretations. Part III shows the conflicts between preservation rules and self-destructing data, as well as where problems might arise in civil litigation.[48] Part IV offers an outlook on how courts should use the Federal Rules to assess this evidence and other potential remedies.

I. BACKGROUND ON SELF-DESTRUCTING DATA APPLICATIONS

A. *Snapchat*

Snapchat was created in a fraternity house by Stanford students Evan Spiegel and Bobby Murphy in April 2011.[49] The two were inspired after hearing stories of social media crises such as emergency untagging of compromising Facebook photos before job interviews.[50] Snapchat was launched in Apple's AppStore in September of 2011.[51] By October 2014, app users were sending 700 million Snaps per day.[52] The program is particularly popular among smartphone users under twenty-five;[53] seventy-seven percent

47. *See* SHIRA A. SCHEINDLIN & DANIEL J. CAPRA, ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE IN A NUTSHELL 63 (2009).

48. This Comment primarily addresses ephemeral data issues that arise during litigation. For a brief analysis of pre-litigation ephemeral data problems, see *id*. at 233-35.

49. Poltash, *supra* note 4, ¶ 10; Evan Spiegel, *Let's Chat.*, SNAPCHAT BLOG (May 9, 2012, 7:11 PM), http://blog.snapchat.com/post/22756675666/lets-chat.

50. Spiegel, *supra* note 49.

51. *Id.*

52. Saitto, *supra* note 3.

53. Poltash, *supra* note 4, ¶ 16.

of college students use the app at least once per day.[54]

From the beginning, Snapchat's creators emphasized the value of ephemeral social media.[55] Snapchat researcher Nathan Jurgenson has written several blog posts about ephemerality, stressing that permanent content is merely "one option."[56] Jurgenson argues that life is a flow of ever-changing events, and not all of them are meant to be "captured, preserved, and put behind glass" like a Facebook profile.[57] He states permanent social media fixates on a photo, while temporary social media focuses on what it meant and how you felt, which more closely mimics the fluidity of life itself.[58] Jurgenson poignantly concludes, "[t]he Web doesn't mean the end of forgetting; indeed, it has demanded it."[59]

Evan Spiegel, CEO of Snapchat, discussed ephemerality and the changing nature of social media in a January 2014 keynote address:

> The selfie makes sense as the fundamental unit of communication on Snapchat because it marks the transition between digital media as self-expression and digital media as communication. And this brings us to the importance of ephemerality at the core of conversation. . . . Snapchat sets expectations around conversation that mirror the expectations we have when we're talking in-person.[60]

The way Snapchat works is simple. Once a user downloads the app and registers a username, the user can allow Snapchat to access phone numbers, easily letting

---

54. Wagner, *supra* note 18.

55. Team Snapchat, *Snapchat Turns 1 Today!*, SNAPCHAT (Sep. 26, 2012, 1:50 PM), http://blog.snapchat.com/post/32347694051/snapchat-turns-1-today.

56. Nathan Jurgenson, *The Liquid Self*, SNAPCHAT BLOG (Sep. 20, 2013, 10:38 AM), http://blog.snapchat.com/post/61770468323/the-liquid-self.

57. *Id.*

58. Nathan Jurgenson, *Temporary Social Media*, SNAPCHAT BLOG (July 19, 2013, 2:43 PM), http://blog.snapchat.com/post/55902851023/temporary-social-media.

59. *Id*.

60. Evan Spiegel, *2014 AXS Partner Summit Keynote*, SNAPCHAT BLOG (Jan. 27, 2014, 11:13 AM), http://blog.snapchat.com/post/74745418745/2014-axs-partner-summit-keynote.

friends become Snapchat contacts.[61] When a user takes a photo, the user can type a line of text over the photo, draw on the photo, and apply various filters.[62] A user chooses exactly which contacts the user wishes to send the Snap to, and the sender can allow the photo to be viewed for one to ten seconds.[63] When a user shoots a video of one to ten seconds, all of the same features apply.[64] When a person receives a Snap, it appears in the Snapchat log, and the recipient touches the message entry and holds a finger down on the touchscreen to view.

The key component of the application is self-deletion.[65] The content is stored in a temporary folder in a smartphone's memory files.[66] This can either occur in internal memory, Random Access Memory (RAM), or external memory.[67] Once a Snap is viewed, the sender can see that the message was viewed, and the temporary copy is deleted from the recipient's phone.[68] The content is also sent to Snapchat servers, and once it has been viewed by all recipients, it is deleted from the servers.[69] An unopened Snap remains on servers for thirty days, at which point it is deleted.[70] The only record that remains is the Snapchat log, which looks like a phone record. The log of fifty[71] entries details who you sent a

---

61. Poltash, *supra* note 4, ¶ 11.

62. *Id.* ¶ 12.

63. *Id.*

64. *Id.*

65. *See* Team Snapchat, *How Snaps Are Stored And Deleted*, SNAPCHAT BLOG (May 9, 2013, 7:23 PM), http://blog.snapchat.com/post/50060403002/how-snaps-are-stored-and-deleted.

66. *Id.*

67. *Id*.

68. *Id*.

69. *Id*.

70. *Id.*

71. While user devices have a log of the last fifty Snaps, Snapchat servers retain a log of the last two hundred Snaps that have been sent and received. *Snapchat Law Enforcement Guide*, SNAPCHAT, https://info.publicintelligence.net/SnapchatLawEnforcementGuide.pdf (last updated Dec. 1, 2012).

Snap to (or who sent you one), the time, and message status (sent, delivered, or opened).

While the purpose of Snapchat is to send content that disappears, photos and videos now have various ways to be saved. When a user creates content, there is a "save" icon that will preserve the content on the user's phone. A user can also choose to add the content to "My Story," which permits friends to view the Snap an unlimited number of times for twenty-four hours. A recipient can screenshot the Snap, which will notify the sender. A new "replay" feature permits a recipient to replay any one Snap per day, which will also notify the sender.[72]

Snapchat expanded its features even further on May 1, 2014. Users can now send text messages through the app, which disappear when both users exit the screen.[73] Screenshots of this content are permitted and will alert the other user, just as photo screenshots do.[74] Further, Snapchat users can utilize two-way and one-way live video chatting through the app.[75] These features provide a tremendous boost in functionality for the increasingly popular app.[76]

However, Snapchat is far from foolproof. As mentioned earlier, a digital forensics firm found a way to re-access Snaps on Android phones at later times, despite claims by Snapchat that the content disappears from the phone.[77] The

---

72. Snapchat has not elaborated on how the "replay" feature reconciles with its promises to delete Snaps from servers and devices immediately after being viewed. When a person finishes viewing a Snap, the option to replay it appears. When you choose to replay, the app informs you that this is a once-per-day feature, then reloads the Snap. However, replay must occur before leaving the application; if you view a Snap and close the application, replay is not available when you return.

73. Stan Schroeder, *Snapchat Adds Video Chat, Instant Messaging*, MASHABLE (May 1, 2014), http://mashable.com/2014/05/01/snapchat-adds-video-chat-instant-messaging. This is a similar feature to what Apple unveiled for its upcoming iOS 8. *See supra* note 28 and accompanying text.

74. Schroeder, *supra* note 73.

75. *Id.*

76. *See id.*

77. *Snapchat Unveiled: An Examination of Snapchat on Android Devices*, DECIPHER FORENSICS (Jan. 23, 2014), http://www.decipherforensics.com/snapchat.

study concluded that metadata are stored for expired and unexpired Snapchat images, and that the images do not disappear forever as Snapchat claims.[78] EPIC filed a formal investigation request to the FTC, alleging deceptive business practices and asking the FTC to force Snapchat to improve its data security practices.[79] This warning rang true months later, when 4.6 million Snapchat usernames and phone numbers were leaked online by a company whose stated purpose was to wake up Snapchat and the public to its security vulnerabilities.[80] Subsequently, EPIC renewed its FTC complaint, faulting both Snapchat's security weakness and the FTC's inaction since EPIC's initial filing.[81] While Snapchat says it takes "reasonable measures" to ensure security,[82] no security measures have been taken since the breach, other than the announcement of a minor app update.[83] Snapchat eventually settled with the FTC over EPIC's complaint; Snapchat will be prohibited from misrepresenting the extent to which it maintains privacy, security, and confidentiality of user information.[84] The

78. *Id.*

79. Cutler, *Privacy Group*, *supra* note 43.

80. Joyce E. Cutler, *Snapchat Announces Security Update Responding to Online Posting of User Info*, BLOOMBERG BNA ELEC. COM. & LAW REP. (Jan. 8, 2014) [hereinafter Cutler, *Security Update*]; Chris Ziegler, *Alleged Snapchat Hackers Explain How and Why They Leaked Data on 4.6 Million Accounts*, THE VERGE (Jan. 1, 2014), http://www.theverge.com/2014/1/1/5263156/alleged-snapchat-hackers-explain-how-and-why-they-leaked-data-on-accounts.

81. *Id*. To date, the FTC has still not responded to EPIC's complaint, other than to say it has been received. *Id.*

82. *Snapchat Privacy Policy*, *supra* note 41. It is worth noting that, despite its highly publicized security issues, Snapchat's privacy policy has exactly one sentence in its "Security" section, its terms of use has one paragraph in its "Account Security" section (which only focuses on what users should not do), and not a single blog post is about security. *Id.*; *Snapchat Terms of Use*, https://www.snapchat.com/terms (last updated Dec. 20, 2013).

83. *See* Cutler, *Security Update*, *supra* note 80.

84. Juan Carlos Rodriguez, *EPIC Pushes FTC For Stronger Snapchat Privacy Pact*, LAW360 (June 11, 2014), http://www.law360.com/articles/547075/epic-pushes-ftc-for-stronger-snapchat-privacy-pact. EPIC thought the deal did not go far enough, continuing its aggressive campaign against companies with privacy shortcomings. *Id.*; *see* Allison Grande, *FTC Steps Up Privacy Enforcement, With*

company must also implement a comprehensive privacy program to be monitored for the next twenty years.[85] A similar settlement was reached with the Maryland Attorney General in a state action against Snapchat for privacy shortcomings.[86]

According to its privacy policy, Snapchat gathers other information from users.[87] Snapchat may collect a username, password, email address, phone number, age, and any other information the user chooses to provide.[88] Snapchat also gathers information about usage, logs, devices, location, cookies, and other tracking technologies.[89] The company claims to use this information for service improvement, software updates, trend analyses, and other incidental purposes.[90] Snapchat states it may share such information "[i]n response to legal process or a request for information if we believe disclosure is in accordance with any applicable law, rule, or regulation."[91]

The purposes for Snapchat continue to grow. Some users document exciting or humorous moments during their day, while others send nearly *every* mundane moment of their day, from eating cereal to working out. High school students use the app during lectures to talk to classmates without teachers knowing. Some use it for more nefarious purposes, such as cheating on tests, sexting, sending crude drawings, and flaunting underage drinking.[92] The supposed

---

No Slowdown In Sight; LAW360 (July 23, 2014), http://www.law360.com/articles/559907/ftc-steps-up-privacy-enforcement-with-no-slowdown-in-sight.

85. Rodriguez, *supra* note 84.

86. Marlisse Silver Sweeney, *Snapchat Settles With Maryland Attorney General*, LAW TECHNOLOGY NEWS (July 10, 2014), http://www.lawtechnologynews.com/id=1202662825225/Snapchat-Settles-With-Maryland-Attorney-General-?slreturn=20150007202538.

87. *Snapchat Privacy Policy*, *supra* note 41.

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.*

92. Poltash, *supra* note 4, ¶¶ 19, 22.

inconsequentiality of Snaps makes it easy for these more immoral uses to be carried out.[93]

B. *Vaporstream*

While Snapchat reigns supreme in younger demographics, Vaporstream has attracted attention in the professional world for its own vanishing communications.[94] The startup was unveiled in 2006 by Void Communications LLC as a complement to email and instant messaging, both of which leave abundant records.[95] Originally, the service was not dependent on businesses, and a subscription cost just $40 per individual per year.[96] Now, Vaporstream markets a premium service for companies, which carries a hefty price tag of up to $25,000 per month for fifty employees.[97] The service was originally designed so that subscribers could only contact other subscribers; now, members may contact non-subscribers, such as an attorney communicating privileged information with a client.[98]

Vaporstream aims to bring the security of a face-to-face conversation to the world of instant communications.[99] The company notes a trade-off between privacy and velocity: the most secure communications are phone and face-to-face conversations that must be scheduled in advance, while emails, texts, and instant messages can be sent and received

---

93. *See id.* ¶¶ 18-22.

94. Browning, *Burn after Reading*, *supra* note 1, at 307.

95. Brian Bergstein, *Messages that go 'poof' after sending them*, ASSOCIATED PRESS (Sept. 24, 2006, 9:40 PM).

96. *Id.*

97. Browning, *Burn after Reading*, *supra* note 1, at 307.

98. Jason Krause, *Vaporstream's Disappearing E-mail Act*, N.J. L.J., Apr. 25, 2011, at 3.

99. *See Why Vaporstream*, VAPORSTREAM, https://www.benegourmet.com/why-vaporstream (last visited Sept. 29, 2014) [hereinafter *Why Vaporstream*] (copies on file with *Buffalo Law Review*). As mentioned earlier, Vaporstream changed its website after this Comment was written. *See supra* note 20; *compare Why Vaporstream*, *supra*, *with Why Vaporstream*, VAPORSTREAM, https://www.vaporstream.com/why_vaporstream (last visited Sept. 29, 2014).

instantly, but run the risk of being recorded and discovered.[100] Vaporstream purports to unite security and speed; in its own trademarked words, "It's safe to hit send again."[101] The site also promotes itself as the best way to steer clear of "an avoidable eDiscovery event," as Vaporstream allegedly does not create Electronically Stored Information (ESI).[102]

When a user sends a message via Vaporstream, the message instantly disappears from the sender's device.[103] Once a recipient opens the message, it vanishes from that device as well.[104] When a user checks the Vaporstream page, the user can see that a person has sent him a message, but once the recipient opens it, the name disappears and only the message is shown.[105] Vaporstream also stresses that its transmissions "cannot be intercepted, copied, forwarded, printed, stored or even traced."[106]

Vaporstream differs from Snapchat in a few important ways. Vaporstream says it does not create ESI or a digital footprint.[107] The content is strictly peer-to-peer, meaning it is never stored on an intermediate server.[108] Instead, it is stored in video RAM, which is highly volatile and constantly being overwritten with new data.[109] Screenshots tying content to one person are impossible because the sender's name and

---

100. *Why Vaporstream*, *supra* note 99.

101. Home Page, VAPORSTREAM, https://www.benegourmet.com (last visited Sept. 29, 2014) [hereinafter *Vaporstream Home Page*] (copies on file with *Buffalo Law Review*). As mentioned earlier, Vaporstream changed its website after this Comment was written. *See supra* note 20; *compare Vaporstream Home Page*, *supra*, *with* Home Page, VAPORSTREAM, https://www.vaporstream.com (last visited Sept. 29, 2014).

102. *Vaporstream FAQ*, *supra* note 20.

103. Browning, *Burn after Reading*, *supra* note 1, at 307.

104. *Id.*

105. Bergstein, *supra* note 95.

106. *Vaporstream FAQ*, *supra* note 20.

107. Browning, *Burn after Reading*, *supra* note 1, at 307; *Vaporstream FAQ*, *supra* note 20.

108. Browning, *Burn after Reading*, *supra* note 1, at 307.

109. Krause, *supra* note 98, at 3.

message never appear on screen at the same time.[110] Further, because a Vaporstream message is never stored on a server like Snaps are, the encrypted messages cannot be intercepted.[111] Vaporstream messages cannot be replayed or saved after viewing.[112] However, the company recently announced a new module called VaporIGM, which saves only transitory messages that some organizations may need to comply with internal audit policies, legal holds, or SEC regulations.[113] Finally, former CEO Jason Howe said Vaporstream is an enterprise application, whereas Snapchat is a consumer application,[114] which may also impact its evidentiary treatment.

C. *Other Ephemeral Communication Programs*

Snapchat and Vaporstream are not alone in the new market of self-destroying data technologies. Wickr uses military-grade encryption to send text, video, voice, and document files that self-destruct after a set period of time.[115] Gryphn serves as an encryption tool for communications and makes it difficult to capture the information via screenshot.[116] Ansa, marketed to "those prone to drunk texting," deletes media from the sender's device, recipient's device, and Ansa servers seconds after being read.[117] Burn Note provides self-destructing email through computer software and mobile apps.[118] TigerText, allegedly inspired by the publicized

---

110. *Vaporstream FAQ*, *supra* note 20.

111. David Hechler, *Electronic Messages that Vanish Without a Trace*, CORPORATE COUNSEL (Apr. 22, 2013).

112. *Vaporstream FAQ*, *supra* note 20.

113. *Vaporstream Announces New Governance Product at LegalTech: Streaming E-Communications Platform Facilitates Transitory Messaging*, P.R. NEWSWIRE, Feb. 4, 2014, *available at* http://www.prnewswire.com/news-releases/vaporstream-announces-new-governance-product-at-legaltech-243497291.html.

114. Hechler, *supra* note 111.

115. Browning, *Burn after Reading*, *supra* note 1, at 306.

116. *Id*.

117. *Id.* at 306-07.

118. *Burning Questions*, *supra* note 21.

infidelity of Tiger Woods,[119] stores content on the application's servers instead of on a recipient's phone.[120] The sender can specify a time period between one minute and five days before deletion.[121] *Time Magazine* referred to it as an "iPhone App for Cheating Spouses."[122]

Fittingly, two self-destructing data applications were unveiled as this Comment was being written. Confide, released on January 8, 2014, aims to be "Snapchat for professionals."[123] The app discourages screenshots in the same way Vaporstream does—the sender's name and the content are never on the same screen at the same time.[124] Confide differs from Snapchat in that it relies on email addresses rather than phone numbers.[125] Secret Square, founded by Vaporstream executive Steve Tarzia, was unveiled on January 24, 2014 for "protecting your future self" by destroying messages after two minutes.[126] Tarzia said the app was conceived out of the growing public awareness of NSA data-mining activities.[127] Furthermore, the aforementioned iOS 8 makeover for iPhones was announced in June 2014.[128]

Ephemeral data appears to be here to stay. One author commented that such applications "inherently demonstrate that disclosures lose their primary utility as social data as

---

119. Yarow, *supra* note 6.

120. Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601, 608 (2013).

121. *Id.*

122. Luscombe, *supra* note 21.

123. Yarow, *supra* note 6.

124. *See id.*

125. Aldrin Calimlim, *Confide In Your Friends Off The Record With This New Ephemeral Messaging App*, APPADVICE (Jan. 9, 2014), http://appadvice.com/appnn/2014/01/confide-in-your-friends-off-the-record-with-this-new-ephemeral-messaging-app.

126. Cox, *supra* note 23.

127. *Id.*; *see also supra* notes 12-15 and accompanying text.

128. *See supra* notes 27-32 and accompanying text.

time passes."[129] The surge in self-destroying data applications for personal and professional purposes demonstrates the uptick in the demand for and desirability of ephemeral media. However, the legal world is still unsure which rules to apply to these applications and how to apply them. Part II looks at the Federal Rules to pinpoint the relevant laws to apply to ephemeral communications.

II. RULES OF PRESERVATION AND SPOLIATION

The Federal Rules of Civil Procedure were amended in 2006 to establish a distinct category of evidence: Electronically Stored Information (ESI).[130] Anticipating an increase in computer usage, the change addressed issues related to preserving, disclosing, and seeking ESI.[131] At that time, however, "social networking was in its infancy and its paradigm-shifting impact on how people communicate and share information was yet to be felt."[132] Accordingly, preservation of such evidence has become a hotly debated topic in the legal community.[133] This Part examines the legal framework of the duty to preserve and spoliation.

A. *Language of Applicable Federal Rules*

Federal Rule of Civil Procedure 26(b)(1) states that "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense" and that "[f]or good cause, the court may order discovery of any

---

129. Hartzog, *supra* note 7, at 1017. This notion is not limited to self-destroying data applications. The European Union is considering creation of a sweeping, controversial privacy right—the "right to be forgotten." Meg Leta Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, J. INTERNET L., Sept. 2013, at 1, 8. The proposed regulation would give persons the right to force erasure of their personal data from the Internet under certain circumstances. *Id.* at 10. Proponents argue for one's right to silence a particularly unsettling past and move forward. *Id*. at 11. Critics call it "rewriting history." *Id.*

130. SCHEINDLIN & CAPRA, *supra* note 47, at 2.

131. Browning, *Burn after Reading*, *supra* note 1, at 274; *see* FED. R. CIV. P. 26 advisory committee's note (2006).

132. Browning, *Burn after Reading*, *supra* note 1, at 274.

133. *See id.*

matter relevant to the subject matter involved in the action."[134] Rule 26(b)(2)(C)(iii) also states courts must limit discovery if "the burden or expense of the proposed discovery outweighs its likely benefit."[135] Rule 34(a) provides for the discovery of ESI "stored in any medium" in a "reasonably usable form," a broad approach designed to encompass future technological advancements.[136] Rule 34(b)(1)(C) permits a party to specify the form of the ESI,[137] while Rule 34(b)(2)(E)(ii) mandates ESI must be produced in a form "in which it is ordinarily maintained or in a reasonably usable form."[138] Such evidence must be in the responding party's possession, custody, or control, or that party must have the legal right to obtain the documents on demand.[139]

While Rule 26(b)(2)(B) states that a party need not produce ESI from sources that are not reasonably accessible, a showing of good cause can compel discovery of this ESI.[140] Factors for courts to consider include: (1) specificity of the discovery request; (2) quantity of information available from other, more easily accessed sources; (3) failure to provide relevant information that once existed but is no longer easily accessible; (4) likelihood of finding relevant information that cannot be obtained from more accessible sources; (5) predictions as to the usefulness of further information; (6) importance of the issues at stake; and (7) each party's resources.[141]

---

134. FED. R. CIV. P. 26(b)(1).

135. FED. R. CIV. P. 26(b)(2)(C)(iii).

136. FED. R. CIV. P. 34(a)(1)(A); FED. R. CIV. P. 34 advisory committee's note (2006).

137. FED. R. CIV. P. 34(b)(1)(C).

138. FED. R. CIV. P. 34(b)(2)(E)(ii).

139. FED. R. CIV. P. 34(a)(1); Columbia Pictures Indus. v. Bunnell, No. CV 06-1093 FMC(JCx), 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. May 29, 2007), at *24-25. For elaboration on the meaning of possession, custody, and control, see SCHEINDLIN & CAPRA, *supra* note 47, at 82-97.

140. FED. R. CIV. P. 26(b)(2)(B); FED. R. CIV. P. 26 advisory committee's note (2006).

141. FED. R. CIV. P. 26 advisory committee's note (2006).

B. *The Duty to Preserve*

An obligation to preserve evidence arises when a party has notice that the information will be relevant to litigation or when the party should have known it would be relevant to future litigation.[142] This may arise from common law, statutes, regulations, or court orders.[143] Determining when a party reasonably should have anticipated litigation can be a challenge for courts.[144] Typically, the determination is based on good faith and a reasonable evaluation of the facts and circumstances.[145] Further, the future litigation must be probable, not just possible.[146] However, a plaintiff's duty to preserve is viewed differently than a defendant's because plaintiffs control when litigation begins and, therefore, necessarily anticipate it.[147] Without a court order, the obligation to preserve is generally not extended to non-parties with knowledge of pending or future litigation, due primarily to the costly endeavor of preserving ESI.[148]

Courts struggle with exactly which kinds of ESI are covered by the duty to preserve.[149] The analysis begins with the presumption that all relevant ESI should be preserved.[150] Factors such as the degree of accessibility and costs to preserve may impact a preservation obligation.[151] However, the Federal Rules indicate that "mere . . . inaccessibility" does not automatically "relieve a party of its preservation obligation."[152] Further, some courts have held a duty to

142. SCHEINDLIN & CAPRA, *supra* note 47, at 36.

143. FED. R. CIV. P. 37 advisory committee's note (2006).

144. SCHEINDLIN & CAPRA, *supra* note 47, at 46.

145. *Id.*

146. *Id.* at 47.

147. *Id.* at 48.

148. *See id.* at 38-39.

149. *See id.* at 53-55.

150. *See id.* at 54 (citing Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003)).

151. SCHEINDLIN & CAPRA, *supra* note 47, at 56-57.

152. *Id.* at 56. Not all courts agree with this interpretation of the Federal Rules. *Id.*

preserve does not impart a duty to keep the data in an accessible format, particularly when doing so would be costly.[153] This guideline is accompanied by a standard of reasonableness under the circumstances, as courts do not require parties to "preserve every shred of paper, every e-mail or electronic document, and every back-up tape."[154] Parties typically receive a presumption of adequate preservation if they act thoughtfully, reasonably, and in good faith to preserve or attempt to preserve information for litigation.[155]

A duty to preserve also arises from properly tailored preservation orders.[156] The requesting party has the burden of demonstrating potential irreparable injury of destroyed evidence.[157] The court in *Columbia Pictures Industries v. Bunnell*[158] articulated a three-part balancing test for issuing a preservation order. Courts should consider: (1) the level of concern the court has for continuing existence and integrity of the evidence without a preservation order; (2) any irreparable harm likely to result to the party seeking preservation; and (3) the capability of the party to maintain the evidence, including the original form, condition, and contents, as well as burdens associated with maintaining such evidence.[159] In 2006, the Conference of Chief Justices articulated four similar factors for courts to consider when an order to preserve ESI is sought.[160] Once there is a threshold

---

153. *See* Best Buy Stores L.P. v. Developers Diversified Realty Corp., 247 F.R.D. 567, 570-71 (D. Minn. 2007); Quinby v. WestLB AG, No. 04 Civ.7406 (WHP) (HBP), 2005 U.S. Dist. LEXIS 35583, at *27 n.10 (S.D.N.Y. Dec. 15, 2005).

154. *Zubulake*, 220 F.R.D. at 217.

155. *See* Carla Walworth et al., *Mobile Business Communications May Result in Litigation Risk*, N.Y. L.J., Mar. 18, 2013, at S2, S11.

156. *See* SCHEINDLIN & CAPRA, *supra* note 47, at 78-80.

157. *See id.* at 79. Again, not all courts agree with this approach. *See id.*

158. No. CV 06-1093 FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *28-29 (C.D. Cal. May 29, 2007).

159. *Id.* at *28-29 (citing Capricorn Power Co. v. Siemens Westinghouse Power Co., 220 F.R.D. 429, 433-34 (W.D. Pa. 2004)).

160. CONFERENCE OF CHIEF JUSTICES, GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY-STORED INFORMATION 9-10 (2006), *available at* http://cdm15574.contentdm.oclc.org/cdm/ref/collection/civil/id/56.

showing that the integrity of the ESI is threatened, courts should consider: (1) the nature of the threat; (2) the potential for irreparable harm to the requesting party; (3) the capability of the responding party to maintain the ESI in its original form, condition, and content; and (4) any physical, technological, or financial burdens created by ordering preservation.[161]

C. *Spoliation*

Federal Rule of Civil Procedure 37 governs when a court may impose sanctions for destruction of evidence.[162] First, three elements are common to all spoliation claims: (1) a duty to preserve must have attached before evidence was destroyed; (2) the accused party must have acted with a culpable state of mind[163]; and (3) the other party must have been prejudiced by the destruction of evidence.[164] Courts may also consider factors such as: (1) the degree of interference with the judicial process; (2) whether lesser sanctions will properly remedy the harm; (3) whether sanctions are necessary for deterrence purposes; and (4) whether a party will be unfairly punished for spoliation caused by an attorney.[165]

Courts may issue a variety of penalties for spoliation.[166] Courts may hold violators in contempt, dismiss a case,[167] render a default judgment, issue an adverse jury instruction, prohibit the party from making certain claims or defenses, bar admission of a piece of evidence, strike pleadings, stay proceedings until the party complies, or order monetary

---

161. *Id.*

162. FED. R. CIV. P. 37.

163. Circuit courts sharply differ on what constitutes a culpable state of mind. *See* SCHEINDLIN & CAPRA, *supra* note 47, at 219-24.

164. *Id.* at 218.

165. *Id.* at 218-19.

166. FED. R. CIV. P. 37.

167. Dismissal is generally viewed as the ultimate sanction. Browning, *Burn after Reading*, *supra* note 1, at 297.

penalties.[168]

Crucially, Rule 37(e) provides an exception for failure to provide ESI.[169] "Absent exceptional circumstances, a court *may not* impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the *routine, good-faith operation* of an electronic information system."[170] Rule 37(e) recognizes that some electronic systems designed to meet a party's needs may include "alteration and overwriting of information, often without the operator's specific direction or awareness."[171] The analysis turns on good faith: "[A] party is not permitted to exploit the routine operation of an information system to *thwart discovery obligations*" for ESI that must be preserved.[172] A court may assess good faith through various factors, such as the steps the party took to comply with a court order or agreement to preserve ESI, or whether the party reasonably believes discoverable information will not be reasonably accessible.[173] Regarding the "routine operation" element, the District Court of Connecticut held that in order to take advantage of the Rule 37(e) preservation exception, the party had "to act affirmatively to prevent the system from destroying or altering [ESI], even if . . . destruction . . . occur[s] in the regular course of business."[174] Further, the court stated the loss of information must be due to a routine electronic system in place *before* litigation.[175]

---

168. FED. R. CIV. P. 37(b); Browning, *Burn after Reading*, *supra* note 1, at 281.

169. FED. R. CIV. P. 37(e). Rule 37(e) was also added in 2006; it was originally Rule 37(f), and has since been changed (it is cited as Rule 37(f) in early case law). FED. R. CIV. P. 37 advisory committee's note (2006); *see* SCHEINDLIN & CAPRA, *supra* note 47, at 218 n.1.

170. FED. R. CIV. P. 37(e) (emphasis added).

171. FED. R. CIV. P. 37 advisory committee's note (2006).

172. *Id.* (emphasis added).

173. *Id.*

174. SCHEINDLIN & CAPRA, *supra* note 47, at 231-32 (quoting Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007)).

175. *See id*. at 232.

D. *Preservation of Ephemeral Data*

Ephemeral data have been treated differently than typical ESI by courts and scholars. Although ephemeral data are not barred from being part of a preservation order, retrieving such data is more difficult than for other kinds of data. The Sedona Principles, citing Rule 26 and *Convolve, Inc. v. Compaq Computer Corp.*,[176] state that the preservation obligation for ephemeral data should not impose "heroic or unduly burdensome requirements."[177]

But some parties have argued that ephemeral data are not ESI at all.[178] In *Columbia Pictures Industries v. Bunnell*, defendants argued that RAM, a type of temporary storage, did not constitute ESI because the data were never stored on their website, nor could it be retrieved or fixed in any tangible form.[179] Relying on the Advisory Committee's Notes to Rule 34, the District Court for the Central District of California rejected defendants' argument and held that RAM constitutes ESI.[180] The court further held that despite the transitory nature of RAM, the data were in the possession, custody, or control of the party.[181] Defendants then argued that production would be tantamount to creating new data, which is prohibited by Rule 34.[182] The court rejected this argument as well, as the temporary data already existed, so

176. 223 F.R.D. 162, 177 (S.D.N.Y. 2004). In *Convolve*, the court rejected sanctions for failure to preserve data on an electronic device where the data were automatically overwritten. *Id.* The court found the defendant had no business to maintain these fleeting data. *Id.*

177. THE SEDONA CONFERENCE, BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 95-96 (2d. ed. 2007).

178. *See, e.g.*, Columbia Pictures Indus. v. Bunnell, No. CV 06-1093 FMC(JCx), 2007 U.S. Dist. LEXIS 46364, at *9-10, 21-22 (C.D. Cal. May 29, 2007).

179. *Id*. at *21-22. RAM was defined in the case as "a computer component in which data and computer programs can be temporarily recorded." *Id.* at *23 (quoting MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993)).

180. *Id.* at *24.

181. *Id.* at *25.

182. *Id.* at *26.

an order requiring preservation thereof was appropriate.[183] However, the court did not impose sanctions for spoliation.[184]

Despite some case law on temporary data, no cases exist about data that is *deliberately* self-destroying. While the Federal Rules were amended to try to keep up with technology,[185] they offer no guidance on how to treat ephemeral communications.[186] The Federal Rules were not designed for this, and they are struggling to keep up. Soon, judges will have to address these significant deficiencies in the law. Part III explains problems that may arise for courts in this area.

III. GAPS IN THE PRESERVATION RULES

The Federal Rules of Civil Procedure leave no doubt that ESI is discoverable and can be subject to a duty to preserve.[187] But what this means for ephemeral data is still uncertain, as the broad language of the Federal Rules leaves considerable room for interpretation. This Part explores how courts have interpreted the language of the Federal Rules in cases involving ESI and social media, then explains why the current body of law is insufficient to cover self-destroying data. This Part also analyzes claims made by Vaporstream and Snapchat regarding their legal standing in this area to highlight these gaps in the law.

A. *Spoliation of Social Media and the* Gatto *Decision*

While no cases have yet assessed ephemeral communications programs, a handful of cases have dealt with spoliation of social media.[188] In the earliest known social networking spoliation case, the District Court of Puerto Rico held that courts will regard spoliation of social media in the

183. *Id.* at *26-27.

184. *Id*. at *55.

185. *See* FED. R. CIV. P. 26 advisory committee's note (2006).

186. *See* FED. R. CIV. P. 26, 34.

187. *See* FED. R. CIV. P. 26, 34 advisory committee's notes (2006).

188. Browning, *Burn after Reading*, *supra* note 1, at 285.

same way as any other kind of evidence destruction.[189] Another District Court in Texas held a defendant's decision to make his Facebook profile private and remove his last name from his band's website constituted spoliation and supported an adverse inference jury instruction; the defendant had been trying to protect his identity after fleeing the scene of a bar fight.[190] Contrastingly, in a case involving trademark-infringing trade dress, a defendant restaurant changed its profile picture, which had contained images of the infringing trade dress.[191] The New Jersey District Court did not impose spoliation sanctions here, noting the unique features of Facebook, where "[a]ctive users often change their pictures weekly."[192] This demonstrates judges can be cognizant of the nature of new technologies and how they are used, which impacts their ultimate rulings.

The holding in *Gatto v. United Air Lines, Inc.*[193] may also provide insight into the ephemeral data preservation problem. In *Gatto*, a personal injury suit, a discovery request was made for Gatto's social media accounts, including his Facebook profile.[194] After initially refusing, Gatto was ordered to give opposing counsel access to his Facebook password.[195] Gatto was later notified by Facebook that an unknown IP address (which turned out to be opposing counsel) was accessing his account; he allegedly became scared that he was being "hacked" and deactivated his profile.[196] Pursuant to Facebook policy, all of Gatto's data

189. Torres v. Lexington Ins. Co., 237 F.R.D. 533 (D.P.R. 2006).

190. *See In re* Platt, No. 11-12367-CAG, 2012 U.S. Dist. LEXIS 5075, at *7-8 (Bankr. W.D. Tex. Oct. 29, 2012); *see also* Browning, *Burn after Reading*, *supra* note 1, at 285-86.

191. Katiroll Co. v. Kati Roll & Platters, Inc., No. 10-3620 GEB, 2011 U.S. Dist. LEXIS 85212, at *9 (D.N.J. Aug. 3, 2011).

192. Browning, *Burn after Reading*, *supra* note 1, at 294 (citing *Katiroll*, 2011 U.S. Dist. LEXIS 85212, at *10-11).

193. Gatto v. United Air Lines, Inc., No. 10-CV-1090-ES-SCM, 2013 U.S. Dist. LEXIS 41909 (D.N.J. Mar. 25, 2013).

194. *Id.* at *3-4.

195. *Id.* at *4.

196. *Id.* at *6-7.

were permanently deleted fourteen days after deactivation.[197] When the defendants moved for spoliation sanctions, Gatto claimed he did not intentionally destroy or suppress evidence, which should defeat any motion for sanctions.[198] The District Court of New Jersey disagreed, holding that even if Gatto did not intend to permanently deprive the defendants of the Facebook data, he did intentionally deactivate his profile and failed to reactivate it before the data were deleted.[199]

The *Gatto* decision marks an expansion of the "culpable state of mind" element of spoliation.[200] Normally, the test for spoliation relies on the party's nefarious intent; the *Gatto* court found intent to spoil irrelevant.[201] This is a more results-oriented analysis of spoliation. Because Gatto effectively caused the deletion of data that was subject to a discovery request, a spoliation sanction (an adverse jury instruction) was appropriate.[202] While *Gatto* is only a district court case, it was cited in two other cases in the months after its release.[203]

Gatto could have significant implications for the use of ephemeral communication programs. Under a duty to preserve, Gatto committed spoliation by deactivating his Facebook account and unwittingly causing deletion of his data.[204] What does that mean for individuals who *intentionally* cause deletion of data by choosing an app like

---

197. *Id.* After the information was permanently deleted, the parties agreed to have Gatto download the information, seemingly unaware the information was in fact gone forever. *Id.*

198. *Id.* at *11-12.

199. *Id.* at *12-14.

200. *See* Michael Schmidt & Cozen O'Connor, *The Duty To Preserve Social Media Information*, JDSUPRA BUSINESS ADVISOR (Apr. 10, 2013), http://www.jdsupra.com/legalnews/the-duty-to-preserve-social-media-inform-80011.

201. *Id.*

202. *See Gatto*, 2013 U.S. Dist. LEXIS 41909, at *14-15.

203. Premier Dealer Servs., Inc. v. Duhon, Nos. 12-1498, 12-2790, 2013 U.S. Dist. LEXIS 166661, at *33 (E.D. La. Nov. 22, 2013); Frazier v. Bed Bath & Beyond Inc., No. 2:10-05398, 2013 U.S. Dist. LEXIS 61185, at *19 (D.N.J. Apr. 30, 2013).

204. *Gatto*, 2013 U.S. Dist. LEXIS 41909, at *11-14.

Snapchat? Using a communication medium you know will destroy the data seems more culpable than what Gatto did. This would be bad news for Snapchat and Vaporstream users. But if litigation arises in this area, ephemeral data users would likely attempt to fall back on the expansive language of the Federal Rules, which could produce an entirely different result.

B. *Broad Language in the Federal Rules and Rule 37(e)*

The Federal Rules of Civil Procedure, specifically its preservation and ESI rules, were constructed broadly to encompass future changes in technology.[205] However, parties using ephemeral communications may try to use this broadness to escape those rules. There are various language choices that could become fertile grounds for debate.

As discussed earlier, ESI stored in any medium in a reasonably usable form is discoverable.[206] Parties are also permitted to specify the form of the ESI.[207] But ESI must be produced in a form "in which it is ordinarily maintained or in a reasonably usable form."[208] For an application like Snapchat, this becomes tricky. Before they are viewed, Snaps are "maintained" as the picture or video content itself. After viewing, however, Snaps are "maintained" in the form of a message log. A party seeking Snaps in discovery may argue a "reasonably usable form" would be the image or video itself, which would likely be gone by then. Which form should a party be allowed to demand during discovery?

Preservation becomes a difficult issue as well. Once parties have a duty to preserve, are they obligated to make all efforts to preserve a Snap or a Vaporstream message? The Federal Rules indicate that inaccessibility does not relieve a party of its preservation obligation.[209] Therein lies the tension between ephemeral communications and preservation: how

205. FED. R. CIV. P. 34 advisory committee's note (2006).

206. FED. R. CIV. P. 34(a).

207. FED. R. CIV. P. 34(b)(1)(C).

208. FED. R. CIV. P. 34(b)(2)(E)(ii).

209. SCHEINDLIN & CAPRA, *supra* note 47, at 56.

can you preserve something you no longer have access to? Should a party be required to screenshot or save all ephemeral data?[210] If a party does not do so, has it failed to act "thoughtfully, reasonably, and in good faith"[211] in preserving ESI?

Analyzing the spoliation language of the Federal Rules also reveals potential problems. The "culpable state of mind" requirement varies widely across courts, but the *Gatto* decision construes the term broadly.[212] Gatto was sanctioned for spoliation for intentionally deactivating his profile and not reactivating it for data collection.[213] For parties under preservation obligations, this could be akin to sending an ephemeral message without first saving it. Do Snapchat and Vaporstream users have a culpable state of mind by merely using the programs and not saving the content they send or receive? The Federal Rules, as drafted, cannot answer this question and many others in the ephemeral data realm.

The primary area of future debate in this area will almost assuredly be the Rule 37(e) exception for failure to provide ESI.[214] While Rule 37(e) has seldom been relied upon in the past,[215] when litigation arises in the ephemeral ESI realm, attorneys seeking to avoid discovery will use this "safe harbor"[216] as ammunition. All kinds of ephemeral data users will try to categorize their actions as use of a "routine, good-faith operation of an electronic system."[217] The elements of

---

210. For Snapchat users, screenshots notify the sender of the message. For recipients to screenshot everything for the sake of preservation would certainly raise some red flags for the sender, which may cause the sender to stop sending Snaps all together.

211. Walworth et al., *supra* note 155.

212. Schmidt & O'Connor, *supra* note 200.

213. Gatto v. United Air Lines, Inc., No. 10-CV-1090-ES-SCM, 2013 U.S. Dist. LEXIS 41909, at *11-14 (D.N.J. Mar. 25, 2013).

214. "Absent exceptional circumstances, a court *may not* impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the *routine, good-faith operation* of an electronic system." FED. R. CIV. P. 37(e) (emphasis added).

215. SCHEINDLIN & CAPRA, *supra* note 47, at 229.

216. *See id.*

217. FED. R. CIV. P. 37(e).

routine operation and good faith will be the main points of contention for courts.

A handful of cases have dealt with the "routine operation" requirement of Rule 37(e). In *Doe v. Norwalk Community College*, the District Court of Connecticut cited two reasons for sanctioning a college that wiped email data from its servers: (1) in order to take advantage of Rule 37(e), a party must act affirmatively to prevent destruction or alteration of information, even if such destruction would occur in the regular course of business (a litigation hold); and (2) a routine system must already be in place for the Rule to apply.[218] This second reason also led a Texas District Court to decline sanctioning a police department that had a preexisting policy of keeping transmissions for ninety days.[219] The reasoning makes sense; parties should not be manufacturing routine deletion systems after a duty to preserve arises.

However, the first reason stated in *Doe*—requiring a party to prevent the deletion of routinely deleted data—provides another problem for ephemeral data users: how should this data be preserved? Would this require a Snapchat user to press the "save" button every time the user sends a Snap, or take a screenshot every time the user receives one? How would this work for Vaporstream, Confide, and other apps that actively discourage screenshots? Ephemeral data programs premise themselves on routine deletion of data, so the only latitude in the "routine operation" element may be expansions like the *Doe* holding.

The Rule 37(e) exception—and perhaps the entire issue of ephemeral data preservation—could turn on good faith. A crucial comment in the Advisory Committee's Notes states: "[A] party is not permitted to exploit the routine operation of

---

218. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007).

219. Escobar v. City of Houston, No. 04-1945, 2007 U.S. Dist. LEXIS 72706, at *49-56 (S.D. Tex. Sept. 29, 2007). Plaintiffs in this case requested preservation in a notice of claim, then alleged the police department violated the preservation obligation because the notice of claim arrived within the ninety-day window. The court held that the notice of claim was not specific enough, and that since the police department preserved all residence it believed to be relevant, sanctions were not appropriate. *Id.*

an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that is required to preserve."[220] While the Advisory Committee says good faith *may* be found where a party takes steps to preserve ESI,[221] the *Doe* decision mandating litigation holds for a finding of good faith has been followed several times.[222] Other courts have developed similar doctrines; the District Court for the District of Columbia held that "this Rule does not exempt a party who fails to stop the operation of a system that is obliterating information that may be discoverable in litigation."[223] Several other cases have aligned with this reasoning.[224] These cases may show a trend toward this particular interpretation of Rule 37(e), which has significant implications in the ephemeral data preservation debate.

If ephemeral data programs are categorized as routine, good-faith operation of electronic systems, the only other way to exclude data transmitted over programs like Vaporstream from Rule 37(e) protection would be to categorize its evidence deletion as an exceptional circumstance. According to the Advisory Committee's Notes, this provision recognizes the need for a court to protect an entirely innocent party requesting discovery against serious prejudice that would

---

220. FED. R. CIV. P. 37 advisory committee's note (2006); *see also* Disability Rights Council v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007).

221. FED. R. CIV. P. 37 advisory committee's note (2006).

222. *See* Slovin v. Target Corp., No. 12-CV-863, 2013 U.S. Dist. LEXIS 31858, at *16 (S.D.N.Y. Mar. 7, 2013); Nicholson v. Bd. of Trs. for the Conn. State Univ. Sys., 2011 U.S. Dist. LEXIS 103094, at *11 (D. Conn. Sept. 12, 2011); Johnson v. Waterford Hotel Grp., Inc., No. 3:09-cv-800, 2011 U.S Dist. LEXIS 103094, at *14 (D. Conn. Jan. 11, 2011); Siani v. State Univ. of N.Y., No. CV09-407, 2010 U.S. Dist. LEXIS 82562, at *15 (E.D.N.Y. Aug. 10, 2010); Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 618 n.19 (S.D. Tex. 2010); Toussie v. Cnty. of Suffolk, No. CV 01-6716, 2007 U.S. Dist. LEXIS 93988, at *20 (E.D.N.Y. Dec. 21, 2007).

223. *Disability Rights Council*, 242 F.R.D. at 146.

224. Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007); *see also* Wollam v. Wright Med. Grp., Inc., No. 10-cv-03104, 2011 U.S. Dist. LEXIS 106768, at *3-6 (D. Colo. Sept. 20, 2011); Major Tours, Inc. v. Colorel, 720 F. Supp. 2d 587, 620 (D.N.J. 2010); Cohen v. City of New York, 255 F.R.D. 110, 122 (S.D.N.Y. 2008).

arise from the loss of potentially important ESI.[225] Could a party seeking sanctions argue—as a last resort—that ephemeral data apps constitute an exceptional circumstance?

Neither the Advisory Committee nor the courts have addressed what exactly constitutes an "exceptional circumstance."[226] The District of Columbia District Court held automatic deletion in an email system was not an exceptional circumstance worthy of spoliation sanctions.[227] This marks one of the few times a court has actually assessed with specificity a claim that a circumstance is exceptional. Generally, courts will only find exceptional circumstances for an "exceptionally prejudicial loss of evidence."[228] At least two authors have argued this gives judges "tremendous discretion" in applying this rule.[229] However, this means little when judges do not actually use the exceptional circumstances provision to justify decisions. In ephemeral data litigation, courts may soon be challenged to define what exceptional circumstances are, and whether use of a program like Snapchat could suffice.

C. *Vaporstream, Snapchat, and Law Enforcement*

The websites for Vaporstream and Snapchat offer their own explanations of each company's legal obligations (or lack thereof) when it comes to discovery.[230] Preparing to use the Federal Rules as ammunition, Vaporstream has stocked up its arsenal by preemptively hiding behind Rule 37(e), using its broad language in marketing.[231] One Frequently Asked Question on Vaporstream's website asks, "Am I guilty of

225. FED. R. CIV. P. 37 advisory committee's note (2006).

226. Nicole D. Wright, Note, *Federal Rule of Civil Procedure 37(e): Spoiling the Spoliation Doctrine*, 38 HOFSTRA L. REV. 793, 818 (2009) (citing Rachel Hytken, *Electronic Discovery: To What Extent Do the 2006 Amendments Satisfy Their Purposes?*, 12 LEWIS & CLARK L. REV. 875, 895 (2008)).

227. *Peskoff*, 244 F.R.D. at 61.

228. SCHEINDLIN & CAPRA, *supra* note 47, at 229.

229. Wright, *supra* note 226, at 818 (quoting Hytken, *supra* note 226, at 895).

230. *See Snapchat Law Enforcement Guide*, *supra* note 71; *Vaporstream FAQ*, *supra* note 20.

231. *See Vaporstream FAQ*, *supra* note 20.

hiding something by even using Vaporstream?"[232] The company's reassuring response:

> Absolutely not. In fact, routine, good faith destruction of electronic and other information under a defensible records and information management program is supported both by case law and the recent changes to the Federal Rules of Civil Procedure, which provides safe harbor from negative inference. Just because Vaporstream does not create a record in the first place, does not make one guilty of spoliation.[233]

Vaporstream is practically calling out Rule 37(e) by name, tipping its hand to indicate how it would handle preservation issues—and all but declaring itself immune from preservation duties and sanctions. Vaporstream's Frequently Asked Questions repeated the language more than once—though this inflammatory language has now been conspicuously removed, as mentioned earlier.[234] Other ephemeral data programs have comparable methods of operation and could similarly attempt to use Rule 37(e) as a shield. Does this contravene the purpose of Rule 37(e)? If a preservation order is issued, who would be at fault: the party who would not keep the evidence, or the party who requested something unreasonable?[235]

Vaporstream's Frequently Asked Questions address other litigation concerns in a similar fashion.[236] Vaporstream states its anti-screenshot technology "negat[es] screen capture discovery."[237] The company also stresses discovery cannot possibly take place because Vaporstream does not create ESI.[238] The site states preservation obligations almost never apply to all communications, and because Vaporstream is like face-to-face conversation, a legal hold situation is

---

232. *Id.*

233. *Id.*

234. *See id.*; *see also supra* notes 20, 99, & 101.

235. Rule 34 requires production of evidence in "a reasonably usable form." FED. R. CIV. P. 34(b)(2)(E)(ii).

236. *Vaporstream FAQ*, *supra* note 20.

237. *Id.*

238. *Id.*

impliedly unlikely.[239] On its home page, Vaporstream touts its service as the best way to steer clear of "an avoidable eDiscovery event."[240] So far, Vaporstream users have seen success in the courts. Lawyers have attempted to introduce evidence of a company's Vaporstream use at least thirty-one times; none have succeeded.[241]

Contrastingly, Snapchat appears to be more agreeable when it comes to legal process. According to Snapchat's Legal Enforcement Guide, the application complies with the Electronic Communications Privacy Act,[242] which mandates disclosure of certain user information in response to legal process.[243] Snapchat may disclose user identity info, login info, and account content in response to subpoenas, court orders, and search warrants.[244] Snapchat also complies with preservation requests for information from active accounts.[245] The application will also disclose info voluntarily if Snapchat believes, in good faith, that an emergency involving danger or serious physical injury to any person requires immediate disclosure of the info.[246] Snapchat can also divulge information with user consent.[247] Presently, all of this information seems to be discoverable.

The intriguing question, however, is whether someone can discover Snaps themselves. Apparently, Snapchat can only access and produce unopened snaps.[248] These also appear to be discoverable. According to Snapchat's blog, between May 2013 and October 14, 2013, approximately one

239. *Id.*

240. *Vaporstream Home Page*, *supra* note 101.

241. Hechler, *supra* note 111.

242. 18 U.S.C. § 2701 (2012).

243. *Snapchat Law Enforcement Guide*, *supra* note 71.

244. *Id.*

245. *Id.*

246. *Id.*

247. *Id.*

248. *See* Schaffer, *supra* note 19.

dozen search warrants resulted in production of unopened[249] Snaps to law enforcement.[250] With 350 million Snaps being sent every day as of October 14, 2013,[251] the percentage of Snaps unveiled for legal purposes during that time period was miniscule. But if users have found ways to access deleted Snaps,[252] are these also discoverable and subject to preservation? Senders certainly would not have known their messages would be intercepted.[253] It is unclear how a court will treat this evidence.

As mentioned earlier, there is one major difference between Vaporstream and applications like Snapchat. While Snaps are stored on an intermediate server, Vaporstream messages are not; the peer-to-peer nature of the communication allows Vaporstream to claim that it does not create ESI at all.[254] If Vaporstream's assertion is correct, would that automatically exempt programs like Vaporstream from electronic discovery and leave apps like Snapchat subject to it? This result seems incongruous.

It is clear that auto-deletion changes how discovery works. Instead of being a business with a routine destruction policy, individuals and companies are utilizing applications whose *business* is to destroy. Therein lies the difference between incidentally ephemeral data (such as RAM) and designedly ephemeral data. The Federal Rules and the courts have only dealt with the former, and Part IV deals with the latter.

---

249. As mentioned earlier, unopened Snaps stay on servers for thirty days. Team Snapchat, *supra* note 65.

250. Schaffer, *supra* note 19.

251. *Id.*

252. *Snapchat Unveiled*, *supra* note 77.

253. It is worth noting that despite Snapchat's many claims of Snap secrecy and integrity, its Privacy Policy contains an ominous warning. "[T]here may be ways to access messages while still in temporary storage on recipients' devices or, forensically, even after they are deleted. You should not use Snapchat to send messages if you want to be certain that the recipient cannot keep a copy." *Snapchat Privacy Policy*, *supra* note 41.

254. Browning, *Burn after Reading*, *supra* note 1, at 307; *Vaporstream FAQ*, *supra* note 20.

IV. ADDRESSING EPHEMERAL DATA PROBLEMS

With the rising popularity of ephemeral data programs, courts will soon have to address discovery questions they do not yet have the answers to. Answers must be gleaned in part from existing authority, but this body of authority is not yet sufficient to manage these new issues. The law must adapt. This Part outlines how courts should treat ephemeral communications and offers other potential remedies to correct the shortcomings of the law in this area.

Preliminarily, courts must determine whether all self-destroying messages are ESI. This impacts whether the Federal Rules apply to these programs at all. Vaporstream strongly asserts its program does not create business records or ESI.[255] However, if programs like Vaporstream are correct in that claim while applications like Snapchat are categorized as ESI, Vaporstream users would evade repercussions despite doing the same deeds that Snapchat users could get sanctioned for. Allowing Vaporstream to avoid sanctions due to its design would produce an absurd result. Further, Vaporstream's claim that it is not ESI because it is never stored on a server is without merit. The content is stored in video RAM, which is highly volatile and constantly overwritten,[256] but it is still "stored" in some meaningful sense. As drafted, the Federal Rules do not yet address this nuance. Until they do, courts should regard all ephemeral data technologies as ESI so the Federal Rules can apply to them.

Similarly, for the purposes of ESI discovery, courts should treat all ephemeral data programs in roughly the same way. Each application operates differently, but the idea of impermanent communications is constant. Vaporstream messages may never be stored on a server like Snaps are, but it would be unjust to regard the programs differently in discovery rulings. Not only would this be an inconsistent application of the Federal Rules, but if Vaporstream was essentially exempted from the Federal Rules, ephemeral data users would flock to it. Imagine the marketing advantage: "Vaporstream, the only messaging service that

255. *Id.*

256. Krause, *supra* note 98.

insulates you from the law." Such a result contravenes the purpose of the Federal Rules. While some cases may turn on a more nuanced detail of an ephemeral data program, the programs should be placed into the same category. This ensures the Federal Rules will apply evenly and appropriately across the ephemeral data realm.

A. *Federal Rules 26 and 34*

Working in conjunction, do Federal Rules 26 and 34 require production of ephemeral data? The first hurdle to producing such evidence is Rule 26(b)(2)(C)(iii), which instructs courts to limit discovery if the burden of producing the evidence outweighs its likely benefit.[257] This Rule must always be taken on a case-by-case basis, as it is specific to what the particular ESI would add to the case. The next barrier is Rule 26(b)(2)(B), stating a party need not produce ESI from sources not reasonably accessible.[258] Getting past this roadblock requires a showing of good cause, which is outlined in seven factors.[259] This also must be dealt with on a case-by-case basis, as the seven factors are fact-specific.

But courts can begin to construct some uniform standards when the analysis reaches Rule 34. Judges must determine whether ephemeral communications can be produced in a "reasonably usable form" and what that form actually is.[260] For self-destroying technologies that keep a log, as Snapchat does, judges can feel secure in allowing discovery of the log at the very least. Like a phone record, it will provide only the identities of the two parties and when they communicated. But Vaporstream and many other programs do not keep logs.[261] The only "reasonably usable" form left is the message itself, which is meant to appear quickly and vanish.[262]

---

257. FED. R. CIV. P. 26(b)(2)(C)(iii).

258. FED. R. CIV. P. 26(b)(2)(B).

259. FED. R. CIV. P. 26 advisory committee's note (2006).

260. FED. R. CIV. P. 34(b)(2)(E)(ii).

261. Browning, *Burn after Reading*, *supra* note 1, at 306-07.

262. FED. R. CIV. P. 34(b)(2)(E)(ii); *Vaporstream FAQ*, *supra* note 20.

This tension is echoed in the Federal Rules themselves. While the Federal Rules say a party need not produce unduly burdensome evidence, the Advisory Committee's Notes stress the language of Rule 34 was constructed broadly "to encompass future developments in computer technology."[263] Where should courts draw the line? Coupled with the Federal Rules' expansive intent, judges should consider how litigating against an ephemeral data user who performs illegal activity without leaving a trace behind would cripple opposing parties. Parties should not be completely immune from discovery and spoliation sanctions merely because they chose Vaporstream over Gmail, or Snapchat over text messaging. Such a result is inequitable, especially because those actors chose ephemeral communications with self-destruction in mind.

For these reasons, judges should continue the expansion of Rule 34 and allow all ephemeral messages to be discoverable ESI.[264] This preserves justice and parity in the discovery phase and aligns with the intent of the Federal Rules to encompass future technologies. This should be done carefully, and parties—on a case-by-case basis—should satisfy most or all of the seven factors for a showing of good cause to compel discovery of ESI.[265] Courts must avoid the prejudice that would result from forbidding self-destroying messages to be put through the analysis in the first place.

B. *Preservation Orders*

If ephemeral ESI is discoverable, then it must also be subject to preservation orders and duties to preserve. This

---

263. FED. R. CIV. P. 34 advisory committee's note (2006).

264. *See* Columbia Pictures Indus. v. Bunnell, No. CV 06-1093, 2007 U.S. Dist. LEXIS 46364, at *28-32 (C.D. Cal. May 29, 2007) (expanding the meaning of ESI to include temporary RAM storage).

265. Factors for courts to consider include: (1) specificity of the discovery request; (2) quantity of information available from other, more easily accessed sources; (3) failure to provide relevant information that once existed but is no longer easily accessible; (4) likelihood of finding relevant information that cannot be obtained from more accessible sources; (5) predictions as to the importance and usefulness of further information; (6) importance of the issues at stake; and (7) each party's resources. FED. R. CIV. P. 26 advisory committee's note (2006).

supports the general interpretation of the Federal Rules that all relevant evidence should be preserved and that "mere . . . inaccessibility does not relieve a party of preservation obligation[s]."[266] But this also must be evaluated on a case-by-case basis, as a party should not be subjected to wholly unreasonable discovery.[267] Importantly, allowing judges to consider ephemeral communications as discoverable ESI can allow them to properly evaluate each case. Without this inclusion, however, self-destroying data are essentially barred from consideration as discoverable evidence.

As mentioned earlier, courts consider a three-part balancing test for issuing preservation orders. Judges consider the: (1) level of concern for the continuing existence and maintenance of the evidence without a preservation order; (2) irreparable harm likely to result from destruction of evidence; and (3) capability of the party to maintain the evidence sought to be preserved.[268] Ephemeral communications primarily impact the first and third factors. Judges should be concerned that the evidence will be erased, as that is what ephemeral data programs are designed to do. Absent efforts to save the content, these factors should almost always weigh in favor of the party seeking the ephemeral communications.

Ephemeral data users would contend that they do not have the ability to maintain the evidence under the third factor. Snapchat users would likely not get very far with this argument. In addition to screenshots, the new save button and "My Story" features have made keeping Snaps easier than ever. For these reasons, a judge should be permitted to order preservation of Snaps. Given Snapchat's new features, saving such data is not unduly burdensome. Many other self-destroying applications permit screenshots, which would be

---

266. SCHEINDLIN & CAPRA, *supra* note 47, at 56.

267. FED. R. CIV. P. 34 advisory committee's note (2006).

268. *Columbia Pictures Indus.*, 2007 U.S. Dist. LEXIS 46364, at *28-29 (citing Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433-34 (W.D. Pa. 2004)). The aforementioned Conference of Chief Justices report echoes similar sentiments regarding when to issue preservation orders. CONFERENCE OF CHIEF JUSTICES, *supra* note 160, at 9-10.

the most universally applicable way to order preservation of ephemeral communications.

But what about programs that discourage screenshots? The sender name and content never appear on the screen at once on Vaporstream and Confide.[269] Taking a screenshot of the message without seeing who sent it may render such evidence inadmissible. Further, courts may regard taking screenshots as an unreasonable endeavor for a producing party to undertake. Vaporstream recently debuted its VaporIGM platform, which saves some transitory messages.[270] But this would not include all Vaporstream messages, so instructing a party to turn over its VaporIGM messages would likely not provide the evidence a party opponent would be looking for.

Ken Withers suggests tweaking the factors listed above for ephemeral data preservation.[271] According to Withers, courts should consider: (1) whether the data are uniquely relevant to the litigation; (2) how the data are treated by the party in the ordinary course of business; (3) whether preservation imposes undue costs or burdens relative to the value of the data; and (4) whether technologies exist to preserve the data.[272] This presents a more tailored, albeit insufficient, solution to preservation of self-destroying data. Firstly, it is unclear how exactly courts would treat the second factor. It is clear the party using ephemeral communications treat them as vanishing messages. Parties are using such programs so that their "ordinary course of business" leaves no trace. On that point, the analysis provides little guidance as to the form of ESI courts can ask parties to preserve. Notwithstanding the ambiguity of the second factor, Withers' suggestions are a small step in the right direction for how courts should assess preservation of ephemeral communications.

---

269. *Vaporstream FAQ*, *supra* note 20; *see* Yarow, *supra* note 6.

270. *Vaporstream Announces New Governance Product at LegalTech: Streaming E-Communications Platform Facilitates Transitory Messaging*, P.R. NEWSWIRE (Feb. 4, 2014, 10:00 AM), http://www.prnewswire.com/news-releases/vaporstream-announces-new-governance-product-at-legaltech-243497291.html.

271. SCHEINDLIN & CAPRA, *supra* note 47, at 64.

272. *Id.* Withers borrows from the language of Federal Rule 34. *See* FED. R. CIV. P. 34(b)(2)(E)(i).

Even Withers' more tailored factors still cannot address how to compel preservation of messages from Vaporstream and similar programs. Even with a broadened definition of ESI and an expansion of preservation rules, some ephemeral communications may simply be impossible to preserve without unduly burdensome efforts. However, if courts stopped the analysis here and concluded Vaporstream and similar types of messages cannot be preserved in any capacity, users could run rampant with potentially unlawful messaging. Courts and opposing parties would be powerless to stop it. For this reason, a more stringent solution is warranted.

C. *Litigation Holds and Cessation of Use*

Under the current body of law on the ephemeral data issue, the most effective way to compel preservation of self-destroying evidence is a litigation hold. This action would have precedential support through cases like the aforementioned *Doe* decision.[273] There, the District Court held failure to issue a litigation hold warranted spoliation sanctions.[274] Litigation holds require parties act affirmatively to prevent destruction of information, even if it occurs in the regular course of business.[275] For self-destroying communications, deletion *is* the regular course of business. Litigation holds cannot bring back data that has already been deleted, but it can prevent evidence from future destruction. However, users will be unsure how to implement a litigation hold while utilizing these programs. Normally, suspension of a routine deletion policy might involve a company halting its own procedures that regularly destroy records or delete emails.[276] But Vaporstream users cannot tell Vaporstream to stop deleting their communications.

One answer here is for a litigation hold to require cessation of all ephemeral technology use. Discontinuing use is the only feasible way for users of programs like Vaporstream to act affirmatively to prevent destruction of

273. *See* Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007).

274. *Id.*

275. *Id.*

276. *See* SCHEINDLIN & CAPRA, *supra* note 47, at 65.

information. This is consistent with the traditional use of a litigation hold. Perhaps there is some room for Snapchat users to continue use, so long as they preserve the information in one of the aforementioned ways. But absent such methods, litigation holds should mandate termination of ephemeral data use.

Opponents may argue changing communication programs would be an undue burden. Courts would have to weigh this burden against the peril resulting from destruction of evidence and how likely this destruction is. The nature of ephemeral data programs should nearly always tip the scale against the party under the litigation hold. The threat to the evidence and the injustice that results from allowing its destruction necessitate as much. Further, it is unlikely that a person or company's sole means of communication is through self-destroying data programs. Switching to their other, less secretive messaging method(s) is likely not an undue burden.

D. *Spoliation and the Rule 37(e) Exception*

Once a judge compels production of ephemeral communications or a litigation hold is instituted, can ephemeral ESI destruction be sanctioned under Rule 37? To date, no court has sanctioned a party for failure to preserve such data.[277] Of the three elements of spoliation, use of ephemeral data programs primarily falls under the second element requiring a culpable state of mind.[278] The determinations of what a culpable state of mind is and whether sanctions are appropriate for ESI destruction differ greatly across federal courts.[279] Again, there is little guidance

---

277. SCHEINDLIN & CAPRA, *supra* note 47, at 63.

278. *See* FED. R. CIV. P. 37.

279. The Fifth, Seventh, and Tenth Circuits require a finding of bad faith to sanction a party for failure to produce ESI. SCHEINDLIN & CARPRA, *supra* note 47, at 223. The Second, Third, D.C., and Federal Circuits have held that negligence is sufficient to establish culpability. *Id.* at 219-21, 223. The Ninth Circuit requires willfulness, fault, or bad faith. *Id.* at 223. The Fourth and Sixth Circuits require willfulness, which is somewhere between negligence and bad faith. *Id.* The Eleventh Circuit varies by case. *Id.* at 224. The Eighth Circuit has required some indication of intent to destroy evidence in order to obstruct the truth. *See id.* The

in the current body of law to determine how a court should treat ephemeral data programs, but as it stands, the Circuits could go in various directions on the issue.

The *Gatto* decision is a timely expansion of the "culpable state of mind" requirement that has practical applications in the ephemeral data debate.[280] Gatto made a choice that caused deletion of Facebook information that was subject to a discovery request.[281] He allegedly did not intend to deprive the opposing party of relevant evidence, but the court found his intent irrelevant.[282] If the *Gatto* reasoning is applied to ephemeral data usage, the result is clear: users of self-destroying technologies possess the requisite culpable state of mind for a finding of spoliation. Snapchat and Vaporstream users are effectively causing the deletion of their data regardless of whether they intend to destroy evidence. Further, if destruction without intent can be sanctioned, deletion with the intent to suppress evidence is also worthy of sanction. If courts align with the District of New Jersey's reasoning, all ephemeral data users would be sanctioned for spoliation, given that the other two spoliation factors[283] are met.

Federal courts may opt for a more stringent standard than *Gatto*. Circuit courts have applied various standards for a finding of a culpable state of mind, including mere negligence, gross negligence, recklessness, bad faith, and intentional misconduct.[284] Depending on the facts of a given case, ephemeral data users could fall into any one of those standards. The Circuits will likely continue to split sharply,

---

First Circuit requires a showing that a party knew of the litigation and the document's potential relevance to that claim. *Id.*

280. *See* Gatto v. United Air Lines, Inc., No. 10-CV-1090-ES-SCM, 2013 U.S. Dist. LEXIS 41909 (D.N.J. Mar. 25, 2013).

281. *Id.* at *4-5.

282. *Id.*

283. These include the party being subject to a duty to preserve before the evidence was destroyed and prejudice upon the other party. SCHEINDLIN & CAPRA, *supra* note 47, at 218.

284. *Id.* at 219.

just as they have in their current definitions of what constitutes a culpable state of mind.[285]

However, courts should adhere to the standard in *Gatto* in the realm of ephemeral data spoliation. The transitory nature of the information and the way the technology is used makes this the appropriate standard of review for ephemeral ESI spoliation. As mentioned earlier, the interest of fairness reigns supreme in preserving ephemeral data, just as it does throughout the existing preservation rules.

Ephemeral data users will almost certainly fight such sanctions on Rule 37(e) grounds. Rule 37(e) states that absent exceptional circumstances, courts may not sanction parties for ESI lost as a result of routine, good-faith operation of an electronic system.[286] The analysis here turns on good faith and exceptional circumstances.

Good faith may be difficult to pin down, while bad faith is relatively easy to demonstrate.[287] A party's active role in deleting data, such as deleting emails or use of wiping software, will be viewed as bad faith.[288] But courts have no uniform standard as to what constitutes good faith. If courts abide by the *Doe* decision, a showing of good faith would require a litigation hold for Rule 37(e) purposes.[289] The deletion of data by ephemeral communication programs constitutes a "routine operation," but under the *Doe* reasoning, a party must step in and stop this operation.[290] As stated earlier, the best way to preserve data transmitted over ephemeral data programs is to simply use other programs. This is the best case scenario for preservation purposes, and litigation holds go a long way toward demonstrating good faith to judges. Parties cannot be "permitted to exploit the routine operation of an information system to thwart discovery obligations" for ESI that must be preserved;[291] this

285. *Id.*

286. FED. R. CIV. P. 37(e).

287. SCHEINDLIN & CAPRA, *supra* note 47, at 230.

288. *See id.*

289. Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007).

290. *Id.*

291. FED. R. CIV. P. 37 advisory committee's note (2006).

is exactly the kind of bad faith Rule 37(e) is designed to prevent.

Courts should align with *Doe* and hold good faith under Rule 37(e) requires a litigation hold. Consequently, a party's choice to use of an ephemeral data program after a duty to preserve arises constitutes bad faith. Parties should not be permitted to withhold items from discovery by using a secret, self-destroying messaging service. Rule 37(e) was meant to protect technology users whose regular computer operations resulted in incidental losses of temporary data;[292] it was not intended to provide a shield for ephemeral data programs to hide behind.

Courts also should not deem these situations to be "exceptional circumstances." While elaboration on the term is minimal in the current body of law, this should be reserved for particularly egregious circumstances where destruction of evidence was extraordinarily prejudicial. Mere involvement of ephemeral data programs does not rise to the level of exceptional circumstances.

When a court orders sanctions on a party for such actions, which are most appropriate in the ephemeral data context? As with most of these rules, this should be determined on a case-by-case basis. Spoliation rulings frequently involve monetary sanctions,[293] which could be appropriate in this context. Dismissal of an entire case is a particularly harsh judgment, especially in the ephemeral data realm, where users may not intend to commit spoliation.[294] Courts have a variety of other sanctions at their disposal, such as barring evidence or striking pleadings, which may be prudent in a particular case.[295]

---

292. *See id*.

293. SCHEINDLIN & CAPRA, *supra* note 47, at 238-39.

294. Generally, when mulling dismissal or default judgment as a sanction, courts consider: (1) the degree of actual prejudice; (2) the amount of interference with the judicial process; (3) culpability; (4) whether the court warned that party of a possible dismissal or default judgment; and (5) the efficacy of lesser sanctions. *Id.* at 236-37.

295. Browning, *Burn after Reading*, *supra* note 1, at 281.

But a more appropriate sanction for ephemeral data users would be an adverse inference jury instruction.[296] Here, a judge may instruct a jury to infer that missing evidence is unfavorable to the party that caused its absence.[297] This is appealing for ephemeral data sanctions for three reasons. First, it permits juries to determine for themselves whether use of self-destroying communications is determinative in a case. U.S. Magistrate Judge Andrew Peck noted that while there is no case law in this area yet, there will be at some point.[298] Someday, Peck submits, there may be an email that suggests that the sender and receiver continue their conversation on Vaporstream, which will not look good to a jury.[299] Second, an adverse inference instruction is a strong sanction that can have beneficial deterrent effects on those who use ephemeral data programs to circumvent the law. Third, it imparts fairness on both parties. For ephemeral data users, it gives them an opportunity to convince a jury their use of a program like Vaporstream was not for nefarious purposes. For the opposing party, it ensures the party does not get off scot-free for violating its preservation obligations.[300]

E. *Other Potential Remedies*

1. *Changes to the Federal Rules.* Because courts are left to interpret a set of rules that have significant gaps, the first and primary remedy should be changes to the Federal Rules of Civil Procedure. As discussed earlier, the Federal Rules were written before ephemeral communications rose in popularity.[301] Because the current Rules are insufficient to guide courts in this new area, they must change to adapt to

296. It is important to note that the proponent of an adverse inference instruction bears the burden of proving the lost evidence would have been relevant. SCHEINDLIN & CAPRA, *supra* note 47, at 237.

297. *Id.*

298. Hechler, *supra* note 111.

299. *Id.*

300. Barclay T. Blair, *Bombs Away; Erasing information in the Big Data era*, 19 LAW TECH. NEWS 62 (Apr. 1, 2013) ("[U]se [of ephemeral data programs] might come with a cost—a possible inference of guilt by association that could be exploited by the other side in litigation.").

301. Browning, *Burn after Reading*, *supra* note 1, at 308.

the times. This can be done either through substantive rule changes or through additions to the Advisory Committee's Notes to clarify vague language.

First, in order to quell any doubts about the nature of ephemeral data, the Federal Rules should reflect the fact that ephemeral communications are ESI. Courts may have already regarded such data as ESI by that time, but placing ephemera in that realm allows it to be undoubtedly subject to ESI discovery rules. Second, the Federal Rules should clarify what it means for evidence to be "ordinarily maintained" and what a "reasonably usable form" is under Rule 34.[302] They need not address programs specifically, but courts need more to work with to determine what exactly is discoverable. Third, preservation rules must address what to do with data that is not meant to be preserved. Courts will be scrambling to balance the current language of the Federal Rules with unjust situations resulting from ephemeral data loss. Judges have no guidance on whether ephemeral ESI is even subject to a preservation order. Finally, the Federal Rules must more directly address which kinds of actions fall into the Rule 37(e) exception. While the exception has been scarcely used to date, courts can assess Rule 37(e) challenges with more clarity and direction before a flood of ephemeral data users attempt to hide behind it. These changes will not necessarily cure the problem, and the Federal Rules should not be exclusionary in their narrowness. But these would provide a basic framework for courts to work with when deciding this new line of cases.

The Federal Rules could also benefit from additional language in the spoliation rules. Elaboration on when parties may be sanctioned—specifically for ephemeral ESI destruction—would also aid courts in figuring out exactly how to assess spoliation situations. The United States Courts' Advisory Committee on Civil Rules has taken a step toward clarifying Rule 37 with a proposed amendment to Rule 37(e).[303] The proposed amendment would split sanctions into two categories: (1) remedies and other curative steps

302. FED. R. CIV. P. 34(b)(2)(E)(ii).

303. Browning, *Burn after Reading*, *supra* note 1, at 280.

short of true sanctions; and (2) typical sanctions courts impose now, such as an adverse inference instruction.[304] Curative steps could include recreating or obtaining lost information, conducting additional discovery to compensate, or pay reasonable expenses resulting from the data loss.[305] Courts would only be permitted to impose sanctions where deletion deprived a party of any meaningful opportunity to litigate its claim, or the failure to preserve caused substantial prejudice and was willful or in bad faith.[306] This provision has been controversial, and its potential adoption hangs in limbo.[307] The proposed amendment could be useful in the ephemeral data realm to more appropriately sanction parties based on their level of culpability. For example, "curative" steps could be appropriate for a Snapchat user who unwittingly captured something of evidentiary significance and let it self-delete. True sanctions would be more suited for the corporate executive who sent insider trading tips on Vaporstream, counting on the self-deletion protocol to absolve him of responsibility.

Another helpful distinction, either in the Federal Rules or in the courts, would be to distinguish inherently ephemeral data from designedly ephemeral data. The former are data that are incidentally erased frequently as a part of another function, such as the RAM of a computer. Designedly ephemeral data are programs like Snapchat and Vaporstream, constructed for the sole purpose of discreet and recordless communications. Setting out the difference could aid courts in determining whether a party has a culpable state of mind or has acted in bad faith in failing to preserve ephemeral data.

2. *Additional Legislative Measures.* The United States Government could pass legislation to restrict the ability of ephemeral data programs to erase all data. If concerns about ephemerality abounded among voters, members of the Legislative Branch could enact reforms to counter the spread

304. *Id.* at 280-81.

305. *Id.* at 281.

306. *Id.* To determine willfulness or bad faith, courts may examine "the extent to which a party was on notice of probable litigation, and/or the reasonableness of a party's efforts to preserve the information that was ultimately lost." *Id.*

307. *See id.*

of the programs. The legislative intent of such laws would likely be watched closely by courts as they determine exactly how to treat this data. Contrastingly, legislation could be adopted that promotes impermanent data. For example, one proposed law, called the Online User Data Expiration Act (OUDEA), would require all U.S. websites that allow users to post self-generated content to provide data destruction technology for such content.[308] Congressional emphasis on promoting impermanence would have significant ramifications for ephemeral data in the courts, likely leading to a loosening of the restrictions on ephemeral data users in litigation suggested in this Comment. Interestingly, ephemeral data companies have begun to hire lobbyists to influence politics in Washington D.C. should any such legislation arise.[309] However, some experts are unsure that legislation for ephemeral data programs would be useful.[310]

3. *Hacking or Recalling Old Deleted Files.* As discussed earlier, Snaps may be recoverable through a hack or by accessing certain folders in the hard drives of Android devices.[311] Further, ephemeral data programs may eventually be subject to hacking breaches, despite their rigorous security encryption measures.[312] What if ephemeral messages never truly disappear? Are these messages discoverable?

Ephemeral data that have been recalled by whatever means should still be discoverable and subject to preservation. If ephemeral data users allow discoverable data to be erased only to recover it later, it should still be usable in a trial. The fact that it is obtained after the fact should not change its treatment in court. In a way, this result is a better outcome for courts and litigants. Not only do you get the evidence back into the case, but a judge and jury can

---

308. Karen Majovski, Comment, *Data Expiration, Let the User Decide: Proposed Legislation for Online User-Generated Content*, 47 U.S.F. L. REV. 807, 818-19 (2013).

309. Warren Communications News, Inc., *Tech Lobbying Seen Pushing for Anti-SLAPP, Data Breach Laws*, WASH. INTERNET DAILY (Jan. 13, 2014).

310. Warren Communications News, Inc., *Snapchat Attack Leaves Experts Divided Over Whether Legislation Would Enhance Data Security*, WASH. INTERNET DAILY (Jan. 6, 2014).

311. *Snapchat Unveiled*, *supra* note 77.

312. Hechler, *supra* note 111.

see exactly what a party may have been attempting to hide by using an ephemeral data program. This allows courts to more accurately assess the spoliation factors to determine the appropriate sanctions.

CONCLUSION

The recommendations of this Comment come down particularly hard on ephemeral data users. This stance is born out of concern for parties lacking evidence to sustain valid claims while ephemeral data users hide behind the very rules designed to protect those parties. The Federal Rules of Civil Procedure were not constructed for this, but this does not mean ephemeral data users should be immune from the law. The Federal Rules are deliberately broad to encompass technological advancements. Judges are often cognizant of how new technologies are used, so they can broadly interpret the Federal Rules to decide cases appropriately based on the specific features of the technology.[313] But ephemeral data users can use that broadness against opposing parties to avoid punishment for letting evidence destroy itself. Until the Federal Rules are clearer on the issue, courts should err on the side of preserving all ephemeral communications and levying sanctions against parties who fail to do so. A contrary result would permit ephemeral data users to escape legal consequences until the Federal Rules are updated in this area, which may never happen at all.

As human interaction changes, the popularity of ephemeral communications will continue to rise. Failure to address the shortcomings in the traditional framework of discovery and evidentiary rules would have dire consequences for the legal system and electronic discovery.

313. *See* Katiroll Co. v. Kati Roll & Platters, Inc., No. 10-3620 GEB, 2011 U.S. Dist. LEXIS 85212 (D.N.J. Aug. 3, 2011).